From the
INTERNATIONAL PRELIMINARY EXAMINING AUTHORITY

To:
PHILIP R. WADSWORTH
QUALCOMM INCORPORATED
5775 MOREHOUSE DRIVE
SAN DIEGO, CA 92121

PCT

WRITTEN OPINION

(PCT Rule 66)

Applicant's or agent's file reference 030010WO	Date of Mailing (*day/mo* REPLY DUE 04 JAN 2005 within 2 months/days from the above date of mailing

International application No.	International filing date (*day/month/year*)	Priority date (*day/month/year*)
PCT/US03/41538	30 December 2003 (30.12.2003)	07 January 2003 (07.01.2003)

International Patent Classification (IPC) or both national classification and IPC

IPC(7): H04L 9/00; H04K 1/00 and US Cl.: 380/ 30, 282, 286

Applicant

QUALCOMM INCORPORATED

1. This written opinion is the first (first, etc,) drawn by this International Preliminary Examining Authority.

2. This opinion contains indications relating to the following items:

- I ☒ Basis of the opinion
- II ☐ Priority
- III ☐ Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- IV ☐ Lack of unity of invention
- V ☒ Reasoned statement under Rule 66.2 (a)(ii) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
- VI ☐ Certain documents cited
- VII ☐ Certain defects in the international application
- VIII ☒ Certain observations on the international application

3. The applicant is hereby **invited to reply** to this opinion.

When? See the time limit indicated above. ~~The applicant may, before the expiration of that time limit, request this Authority to grant an extension. See rule 66.2(d).~~

How? By submitting a written reply, accompanied, where appropriate, by amendments, according to Rule 66.3. For the form and the language of the amendments, see Rules 66.8 and 66.9.

Also For an additional opportunity to submit amendments, see Rule 66.4.
For the examiner's obligation to consider amendments and/or arguments, see Rule 66.4 *bis*.
For an informal communication with the examiner, see Rule 66.6

If no reply is filed, the international preliminary examination report will be established on the basis of this opinion.

4. The final date by which the international preliminary examination report must be established according to Rule 69.2 is: 07 May 2005 (07.05.2005)

Name and mailing address of the IPEA/US Mail Stop PCT, Attn: IPEA/US Commissioner for Patents P.O. Box 1450 Alexandria, Virginia 22313-1450 Facsimile No. (703) 305-3230	Authorized officer Gilberto Barron Peggy Harwood Telephone No. 703-305-3900

Form PCT/IPEA/408 (cover sheet)(July 1998)

I. Basis of the opinion

1. With regard to the **elements** of the international application:*

☒ the international application as originally filed

☒ the description:
pages 1-15, as originally filed
pages NONE, filed with the demand
pages NONE, filed with the letter of _____.

☒ the claims:
pages 16-25, as originally filed
pages NONE, as amended (together with any statement) under Article 19
pages NONE, filed with the demand
pages NONE, filed with the letter of _____.

☒ the drawings:
pages 1-5, as originally filed
pages NONE, filed with the demand
pages NONE, filed with the letter of _____.

☐ the sequence listing part of the description:
pages NONE, as originally filed
pages NONE, filed with the demand
pages NONE, filed with the letter of _____.

2. With regard to the **language**, all the elements marked above were available or furnished to this Authority in the language in which the international application was filed, unless otherwise indicated under this item.
These elements were available or furnished to this Authority in the following language _____ which is:

☐ the language of a translation furnished for the purposes of international search (under Rule23.1(b)).

☐ the language of publication of the international application (under Rule 48.3(b)).

☐ the language of the translation furnished for the purposes of international preliminary examination(under Rules 55.2 and/or 55.3).

3. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, the written opinion was drawn on the basis of the sequence listing:

☐ contained in the international application in printed form.

☐ filed together with the international application in computer readable form.

☐ furnished subsequently to this Authority in written form.

☐ furnished subsequently to this Authority in computer readable form.

☐ The statement that the subsequently furnished written sequence listing does not go beyond the disclosure in the international application as filed has been furnished.

☐ The statement that the information recorded in computer readable form is identical to the written sequence listing has been furnished.

4. ☒ The amendments have resulted in the cancellation of:

☒ the description, pages None

☒ the claims, Nos. None

☒ the drawings, sheets/~~fig~~ None

5. ☐ This opinion has been drawn as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed, as indicated in the Supplemental Box (Rule 70.2(c)).

** Replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this opinion as "originally filed."*

WRITTEN OPINION

V. Reasoned statement under Rule 66.2(a)(ii) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. STATEMENT

Novelty (N)	Claims	4,7,9,10,12,13,20,21,25,27 and 28	YES
	Claims	1-3,5,6,8,11,14-19,22-24,26 and 29-49	NO
Inventive Step (IS)	Claims	4,7,9,10,12,13,20,21,25,27 and 28	YES
	Claims	1-3, 5, 6, 8, 11, 14-19, 22-24, 26 and 29-49	NO
Industrial Applicability (IA)	Claims	1-49	YES
	Claims	NONE	NO

2. CITATIONS AND EXPLANATIONS

Please See Continuation Sheet

VIII. Certain observations on the international application

The following observations on the clarity of the claims, description, and drawings or on the questions whether the claims are fully supported by the description, are made:

Supplemental Box
(To be used when the space in any of the preceding boxes is not sufficient)

TIME LIMIT:
The time limit set for response to a Written Opinion may not be extended. 37 CFR 1.484(d). Any response received after the expiration of the time limit set in the Written Opinion will not be considered in preparing the International Preliminary Examination Report.

V. 2. Citations and Explanations:

Claims 1, 11, 14, 19, 22, 26, 29-49 and lack novelty under PCT Article 33(2) as being anticipated by Matyas et al (5,201,000; hereinafter Matyas).

Regarding claims 1, 11, 14, 19, 22, 26, 29 and 36, Matyas discloses a method for managing a public key cryptographic system which includes a public key, private key pair generator (abstract). Matyas further discloses generation of a specific public key pair for the purpose of authentication (col. 20, lines40-67; col. 22, lines 45-66). Matyas also discloses the generated keys are transported or transmitted to a receiver (col. 3, line 43-col. 4, line 51; col. 17, lines 4-18). Matyas discloses data processors for processing cryptographic services and usage of random numbers as nonces in authentication protocols (col. 8, lines 58-65; col. 14, lines 61-65). This provides a capability for using a second public key for authentication if a first public key fails.

Regarding claims 30-33, 37-40 and 43-47, Matyas discloses a cryptographic facility (CF) that receives data parameters and encryption key to produce a new set of encrytion keys (col. 9, lines 14-65). Matyas further discloses that the produced public key are used for authentication purpose (col. 20, lines 41-67). Matyas also discloses the use of a counter or a sequence number in the production of the public key set (col. 9, lines 60-66, col. 15, lines 4661). Matyas discloses data processors for processing cryptographic services and usage of random numbers as nonces in authentication protocols (col. 8, lines 58-65; col. 14, lines 61-65). This provides a capability for using a second public key for authentication if a first public key fails.

Regarding claims 34, 35, 41, 42, 48 and 49, these claims are rejected as applied to like elements of claims 30-33 and furtrher the following:
Matyas discloses a technique for selecting a randum number for the purpose of generating a public key set by testing large numbers for primality (col. 13, lines 18-39). This technique is based on the randum number raised to a power chosen from the same series of values that contains the selected randum number.

Claims 2, 3, 5, 6, 8, 15-18, 23 and 24 lack an inventive step under PCT Article 33(3) as being obvious over Matyas et al (5,201,000; hereinafter Matyas) in view of Brennan et al (5,675,649; hereinafter Brennan).

Supplemental Box
(To be used when the space in any of the preceding boxes is not sufficient)

Regarding claim 2, 15 and 23, Matyas does not expressly disclose the creation of two shares of a public key. Brennan, however, teaches that a key is split into shares and each share is given to an agent (see, for example, col. 4, lines 45-520). It would have not involved an inventive step at the time the invention that to include the process of splitting the keys into shares as taught in Brennan in Matyas, because it would requires a minimum number of agents to be present in order to reconstruct the key (Brennan, col. 3, lines 48-55).

Regarding claims 3, 5, 6, 8, 16-18 and 24, Matyas discloses that different types of public key, private key pairs are generated and re-generated by a key generator and transported or transmitted to a receiver (col. 3, line 43-col. 4, line 51; col. 17, lines 4-18). Matyas discloses that a passphrase is used to generate a second type of the public key, private key pairs (col. 4, lines 33-51). Thus, the generated private keys of the second type are associated by the passphrase. Matyas discloses data processors for processing cryptographic services and usage of random numbers as nonces in authentication protocols (col. 8, lines 58-65; col. 14, lines 61-65). This provides a capability for using a second public key for authentication if a first public key fails.

Claim 4 meets the criteria set out in PCT Article 33(2)-(3), because the prior arts do not teach or fairly suggest "disabling the first private key when the second private key is used for authentication".

Claim 7 meets the criteria set out in PCT Article 33(2)-(3), because the prior arts do not teach or fairly suggest "disabling use of the second private key for authentication; and re-creating the second private key and using the second private key for authentication".

Claims 9 and 10 meet the criteria set out in PCT Article 33(2)-(3), because the prior arts do not teach or fairly suggest "disabling use of the second private key for authentication; and using the third private key for authentication".

Claim 12 meets the criteria set out in PCT Article 33(2)-(3), because the prior arts do not teach or fairly suggest "receiving a third public key associated with the second public key, if the first public key fails and if the second public key results in a successful authentication".

Claim 13 meets the criteria set out in PCT Article 33(2)-(3), because the prior arts do not teach or fairly suggest "receiving a third public key and a fourth public key associated with the second public key, if the first public key fails and if the second public key results in a successful authentication".

Claim 20 meets the criteria set out in PCT Article 33(2)-(3), because the prior arts do not teach or fairly suggest "means for receiving a third public key associated with the second public key, if the first public key fails and if the second public key results in a successful authentication".

Claim 21 meets the criteria set out in PCT Article 33(2)-(3), because the prior arts do not teach or fairly suggest "means for receiving a third public key and a fourth public key associated with the second public key, if the first public key fails and if the second public key results in a successful authentication".

Claims 25 meets the criteria set out in PCT Article 33(2)-(3), because the prior arts do not teach or fairly suggest "a set of code segments for disabling the first private key by using the second private key for authentication".

Claim 27 meets the criteria set out in PCT Article 33(2)-(3), because the prior arts do not teach or fairly suggest "a set of code segments for receiving a third public key associated with the second public key, if the first public key fails and if the second public key results in a successful authentication".

Supplemental Box
(To be used when the space in any of the preceding boxes is not sufficient)

Claim 28 meets the criteria set out in PCT Article 33(2)-(3), because the prior arts do not teach or fairly suggest "a set of code segments for receiving a third public key and a fourth public key associated with the second public key, if the first public key fails and if the second public key results in a successful authentication".

Claims 4, 7, 9, 10, 12, 13, 20, 21, 25, 27, 28, meet the criteria set out in PCT Article 33(4), and thus meet industrial applicability because the subject matter claimed can be made or used in industry.